

UNCLASSIFIED

DCI/ICS 85-4060
10 May 1985

MEMORANDUM FOR: Deputy Director of Central Intelligence

VIA: Director, Intelligence Community Staff

FROM: Chairman, Information Handling Committee *EAB*

STAT

SUBJECT: Response to DDCI Questions Regarding OMB Budget
Activities Under NSDD-145

1. This memorandum is provided in response to your request for further information regarding OMB activities carried out under the authority of NSDD-145, which was highlighted in the Information Handling Committee's (IHC) March input to the monthly NFIB Committee reports.

2. NSDD-145 was signed by the President on 17 September 1984 and includes the following language under paragraph 9b, Additional Responsibilities:

"The Director, Office of Management and Budget shall:

Specify data to be provided during the annual budget review by the departments and agencies on programs and budgets relating to telecommunications systems security and automated information systems security of the departments and agencies of the government.

Consolidate and provide such data to the National Manager via the Executive Agent.

Review for consistency with this Directive, and amend as appropriate, OMB Circular A-71 (Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the subject matter herein."

3. OMB worked very hard in the final review process to insure that this language was included in the signed NSDD-145. Immediately after the NSDD-145 was signed, OMB began working on a draft of an OMB bulletin which is intended to provide instructions on "submission of data pertaining to agency programs and budgets for security of automated information systems (computers) operated and maintained by an agency, and by contractors on behalf of an agency." Arnie Donahue, who is the director of OMB's division responsible for monitoring the NFIP and budget, is OMB's representative to the National Telecommunications and Information Systems Security Committee (NTISSC) and leads OMB's efforts in this area.

DCI
EXEC
REG*B-212*
VC B-206

4. OMB Bulletin No. 85-11 (Tab A), dated 28 March 1985, has been issued as a result of OMB's efforts under NSDD-145 with instructions to respond with the submission of data by 28 June 1985. The apparent purposes for which the data is to be collected are set out in Tab B. The data requested includes government owned agency computers as well as contractor installations operated on behalf of an agency. George Rogers, Vice Chairman, IHC, passed consolidated comments on the bulletin to OMB including a strong recommendation to cut down on the data requested and to extend the response time from 60 to 180 days. OMB did cut down on the number of questions it had in its earlier draft and extended the reporting response date to 90 days. It noted that, since the National Security Division would be getting the responses (which could be appropriately classified), no agency would be exempted from responding on the basis of security. The information requested by OMB includes the following:

- number of computer installations processing information classified higher than SECRET;
- number of computer installations processing information classified SECRET or lower;
- type of equipment used at each installation;
- number of computer installations with current valid risk evaluations and accreditations on file and the number of risk evaluations and accreditations in progress;
- forecasts of the number of computer installations for each fiscal year from FY86 to FY90; and
- forecasts of the amount of resources to be obligated by the agency for the security of computer installations for the period 1985-1990 in areas such as: personnel salaries, procurement of computer security protection devices, acquisition of software, physical security of computer installations, and maintenance.

5. Initial reaction to the OMB bulletin was negative because of the amount of effort required to provide to the data OMB has requested. DIA representatives initially reported that DOD would not respond, but Don Latham apparently is now pressing all of DOD to comply with the bulletin. The NTISSC Secretariat at NSA has drafted a more detailed "data call" that it proposes to issue via the NTISSC if the OMB effort does not receive responses from all the agencies. There are indications that agency submissions to OMB will be released to a working group of the SAISS responsible for writing the report on the status of the security of automated information systems in the Federal government which is due in January 1986. This working group includes the SAISS representatives from the IC Staff, CIA, DIA, and NSA.

6. We will keep you informed of the status of the foregoing efforts.

STAT

Attachments: a/s

**SUBJECT: Response to DDCI Questions Regarding the OMB Budget
Activities Under NSDD-145**

Distribution: DCI/ICS 85-4060

Orig - DDCI

1 - Executive Registry

1 - D/ICS

1 - ExSec/NFIB

1 - ICS Registry

1 - ICS Registry

1 - IHC Subject

1 - IHC Chrono

25X1 ICS/IHC/ (10 May 85)



**EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503**

17 APR 1985

LOGGED

March 28, 1985

BULLETIN NO. 85-11

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

**SUBJECT: Data on Security of Automated Information
Systems That Process Information Related to
the National Security Interest**

1. Purpose. This bulletin provides instructions on submission of data pertaining to agency programs and budgets for security of automated information systems (computers) operated and maintained by an agency, and by contractors on behalf of an agency, to process information related to the national security interest.

2. Background. A National Security Decision Directive, National Policy on Telecommunications and Automated Information Systems Security (hereafter referred to as the NSDD), was signed by the President on September 17, 1984. This directive assigns the Director of OMB responsibility to:

a. Specify data to be provided during the annual budget review by the departments and agencies on programs and budgets relating to automated information systems security of the departments and agencies of the government.

b. Consolidate and provide such data to the Secretary of Defense and the Director, National Security Agency in their roles as Executive Agent and National Manager under the NSDD.

This bulletin is being issued to carry out those responsibilities.

3. Scope of initial submission. The NSDD defines two categories of national security information requiring security and protection. They are:

a. Classified information;

b. Other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest.

Information to be submitted under this bulletin will cover only programs and budgets for security of computers that process classified information. This focus on classified information only, as a first step, is intended to provide sufficient time to develop an operational definition of unclassified-but-sensitive information relating to national security--before requiring agencies to submit data on programs and budgets for security of computers that process such information.

4. Definitions. For purposes of this bulletin, the terms used below have the following meanings:

a. Computer installation--A computer installation means a data processor and associated input and output devices that perform the following functions:

- Receive information electronically;
- Process such information;
- Create products (i.e., reports, analyses, etc.) based on such processed information.

Such functions can be performed, for example, by a stand-alone personal computer or by a mainframe computer with many peripheral work stations. Each such computer is considered an installation for purposes of this bulletin. More specifically, computer installations are classified as:

- Microcomputers used as word processors;
- Microcomputers used as personal computers;
- Minicomputers and other microcomputers;
- Mainframes and associated peripherals.

For purposes of this bulletin, a computer that is used as a switching device to route communications is not considered a computer installation. Embedded computers in weapon systems are also to be excluded.

b. Risk evaluation--A risk evaluation means any document which contains an evaluation of the vulnerabilities of a computer installation to the compromise of classified national security information. Such an evaluation should reflect the administrative, physical access, personnel, environmental, technical and communications safeguards installed to prevent a compromise. Such an evaluation could be an in-depth analysis of the security vulnerabilities of a large, specialized computer installation (the kind of evaluation described as a "risk analysis" by OMB Circular No. A-71), or it could be a less intensive examination of security vulnerabilities using less rigorous criteria for a smaller computer installation (such as a microcomputer used as a word processor). Both kinds of vulnerability assessments, if documented, could qualify as risk evaluations under this bulletin. A risk evaluation document can apply to more than one computer installation operated by an agency or by contractors on behalf of an agency. However, such multiples risk evaluations will identify each included computer installation.

c. Accreditation of security for a computer installation--An accreditation of security for a computer installation means a document granting authorization and approval to a computer installation to process classified information in an operational environment. Such authorization and approval is made on the basis of a technical evaluation by designated technical personnel that establishes the extent to which the computer installation design and implementation meet a prespecified set of security requirements. The accreditation document must be signed by a responsible official of the agency. An accreditation document can apply to more than one computer installation operated by an agency or by contractors on behalf of an agency. However, such multiple accreditations will identify each included computer installation.

d. Computer security obligations--Computer security obligations mean dollar amounts within an agency's budget obligated, or to be obligated, for salaries, goods, and services that are primarily intended to improve security of computer installations. Such computer security obligations do not include those for security features that are integral (i.e., built-in) to hardware or software and that cannot readily be removed.

5. Required materials. Agencies will provide the required information, in accordance with the instructions contained in the attachment and in the formats of Exhibits 1, 2, and 3. Negative reports are required. Agencies may classify their submissions at the appropriate level of security classification.

6. Timing of submissions. Agencies will submit the required materials to OMB, Attention: National Security Division, by June 28, 1985.

7. Information contact. Further information may be obtained from Robert S. Dotson (202) 395-4800.


David A. Stockman
Director

Attachment

Attachment
OMB Bulletin 85-11

Instructions for Preparing Submissions in
the Formats of Exhibits 1, 2 and 3
on Computer Security Data

EXHIBIT 1

a. Column 1--1985. Entries in this column are the numbers of computer installations operated and maintained by your agency that currently process classified information--grouped in terms of:

- a. Type of information processed (i.e., higher than Secret or no higher than Secret).
- b. Type of equipment (i.e., microcomputers used as word processors, microcomputers used as personal computers, minicomputers and other microcomputers, and mainframes and associated peripherals).

A particular computer installation will be counted only once. For example, a word processor that is used to process both Top-Secret and Secret information would be counted only once--in the first entry of column 1 (within the number 516 in the attached example Exhibit 1).

b. Column 2--Computer Installations with Currently Valid Accreditations. Entries in this column reflect the extent to which an agency has a formal program of computer-security accreditation meeting the criteria described earlier under the definitions section of this bulletin. Entries in this column will show the number of computer installations listed in Column 1 that have currently valid accreditations of security on file. In the attached example Exhibit 1, 416 of the 516 word processors processing information classified higher than Secret have currently valid security accreditations on file. An accredited computer installation will be counted only once.

c. Column 3--Computer Installations with Accreditations in Progress. Entries in column 3 will show the number of computer installations corresponding to those in column 1 with security accreditations in progress. In the attached example Exhibit 1, 100 of the 516 word processors processing information, classified higher than Secret, have security accreditations in progress. A computer installation with a security accreditation in progress will be counted only once.

d. Column 4--Computer Installations with Currently Valid Risk Evaluations. Entries in column 4 will reflect the extent of an agency's risk evaluation program and will show the number of computer installations, corresponding to the entries of column 1, that have currently valid risk evaluations on file meeting the criteria described in the definitions section of this bulletin. In the attached example Exhibit 1, 420 of the 516 word processors processing information classified higher than Secret have risk evaluations on file meeting such criteria. A computer installation with a currently valid risk evaluation will be counted only once.

e. Column 5--Computer Installations with Risk Evaluations in Progress. Entries in column 5 will show the number of computer installations, corresponding to the entries of column 1, without a currently valid risk evaluation on file, but with such a risk evaluation in progress. In the attached example Exhibit 1, 96 of the 516 word processors processing information classified higher than Secret do not have currently valid risk evaluations on file, but have such risk evaluations in progress. A computer installation with a risk evaluation in progress will be counted only once.

f. Columns 6 through 10--1986, 1987, 1988, 1989, 1990. Entries in these columns will show the numbers of computer installations within the agency in President's budget for 1986 (including estimates for later years). In the attached example Exhibit 1, word processors processing information classified higher than Secret are forecasted to grow from 516 to 642 in 1986. Outyear forecasts for 1987 through 1990 in the 1986 President's budget reflect further growth to 780 such word-processor installations by 1990. A computer installation will be counted only once per column.

EXHIBIT 2

a. Columns 1 through 5. Entries in these columns will display information on computer installations, accreditations and risk evaluations as provided in the instructions for completion of Exhibit 1 (above), but these data will be limited to computer installations that process classified information--and that are operated and maintained by contractors on behalf of an agency.

b. Columns 6 through 10. Entries in these columns will show the best estimates that the responding agency can provide for numbers of computer installations, by type, to be operated and maintained in the future by contractors to process classified information on behalf of an agency.

EXHIBIT 3

Columns 1 through 6--1985 through 1990. Provide estimates of the amounts to be obligated by the agency (in thousands of dollars) for the security of computer installations processing classified information--as reflected in the President's 1986 budget for the period 1985-1990. These estimates of obligations will be limited to computer security programs within the agency. To the extent that efforts to secure classified information are part of a larger program to prevent unauthorized use of information processed on the agency's computers, show only the obligations incurred within that larger program total for computer security of classified information. These amounts should reasonably reflect the numbers of computers, accreditations and risk evaluations listed in your agency's reply to this bulletin in the format of Exhibit 1-- in relation to total agency levels for all computers, accreditations and risk evaluations.

EXHIBIT 3
OMB Bulletin No. 85-11Agency Contact: _____
Phone: _____
Date: _____Obligations for Computer
Security of Classified Information
Department of Government
(Obligations in Thousands)

	<u>1985</u> (1)	<u>1986</u> (2)	<u>1987</u> (3)	<u>1988</u> (4)	<u>1989</u> (5)	<u>1990</u> (6)
Salaries and benefits of computer security administrators and specialists	2150.2	2040.1	2042.1	2050.4	2053.7	2055.0
Procurement of computer security protective devices	200.3	1621.7	300.0	310.0	320.0	330.0
Acquisition of computer security software (development and procurement)	500.7	821.6	605.7	500.0	400.0	300.0
Physical security of computer facilities	100.9	151.9	228.1	150.0	155.0	160.0
Other operations and maintenance for computer security	<u>0.0</u>	<u>0.0</u>	<u>0.0</u>	<u>0.0</u>	<u>0.0</u>	<u>0.0</u>
Total obligations for computer security of classified information	2952.1	4635.3	3175.9	3010.4	2928.7	2845.0

EXHIBIT 2
OMB Bulletin No. 85-11Agency Contact: _____
Phone: _____
Date: _____Contractor Computers Processing Classified Information
on behalf of
The Department of Government

Number of Computer Installations that Process Information Classified Higher than Secret:	1985	Computer Installations with Computer Security Accreditations		Computer Installations with Risk Evaluations		1986	1987	1988	1989	1990
	(1)	Currently Valid (2)	In Progress (3)	Currently Valid (4)	In Progress (5)	(6)	(7)	(8)	(9)	(10)
Microcomputers used as word processors	126	57	69	120	6	130	135	140	140	140
Microcomputers used as personal computers	48	23	25	41	7	50	55	60	65	70
Minicomputers and other microcomputers	4	2	2	4	0	5	6	7	7	7
Mainframes and associated peripherals	1	1	0	1	0	1	1	2	2	2
Numbers of Computer Installations that Process Information Classified No Higher than Secret:										
Microcomputers used as word processors	539	275	264	483	56	550	560	570	580	590
Microcomputers used as personal computers	171	107	64	157	14	180	190	190	190	190
Minicomputers and other microcomputers	26	17	9	21	5	28	30	30	30	30
Mainframes and associated peripherals	5	4	1	5	0	5	5	6	6	6
Total	920	486	434	832	88	949	982	1005	1020	1035

EXHIBIT 1
OMB Bulletin No. 85-11Agency Contact: _____
Phone: _____
Date: _____Computers Processing Classified Information
within
The Department of Government

Numbers of Computer Installations that Process Information Classified Higher than Secret:	1985	Computer Installations with Computer Security Accreditations		Computer Installations with Risk Evaluations		1986	1987	1988	1989	1990
	(1)	Currently Valid	In Progress	Currently Valid	In Progress	(6)	(7)	(8)	(9)	(10)
		(2)	(3)	(4)	(5)					
Microcomputers used as word processors	516	416	100	420	96	642	710	750	770	780
Microcomputers used as personal computers	125	125	0	125	0	156	160	160	160	160
Minicomputers and other microcomputers	8	6	2	8	0	8	8	8	8	8
Mainframes and associated peripherals	2	0	2	2	0	2	2	2	2	2
Numbers of Computer Installations that Process Information Classified No Higher than Secret:										
Microcomputers used as word processors	1000	634	366	770	230	1257	1340	1370	1400	1400
Microcomputers used as personal computers	226	225	1	226	0	327	350	350	350	350
Minicomputers and other microcomputers	50	45	5	50	0	53	53	53	53	53
Mainframes and associated peripherals	7	7	0	7	0	7	7	7	7	7
Total	1934	1458	476	1608	326	2452	2630	2700	2750	2760

**Resource Review Responsibilities and
Authority Specified in NSDD-145**

The purposes for the collection and consolidation of the requested data by OMB and the provision of the consolidated data to the Executive Agent (SecDef) and the National Manager (DIRNSA) are:

- o To support the responsibilities of the Systems Security Steering Group to:*

"Review consolidated resources program and budget proposals for telecommunications systems security, including the COMSEC Resources Program, for the US Government and provide recommendations to OMB for the normal budget review process. (NSDD-145, 4a(4))

"Review in aggregate the program and budget proposals for the security of automated information systems of the departments and agencies of the government." (NSDD-145, 4a(5))

- o To support the Executive Agent in his responsibility to:*

"Review and assess for the Steering Group the proposed telecommunications systems security programs and budgets for the departments and agencies of the government for each fiscal year and recommend alternatives, where appropriate. The views of all affected departments and agencies shall be fully expressed to the Steering Group. (NSDD-145, 6f)

"Review for the Steering Group the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for each fiscal year." (NSDD-145, 6g)

- o To support the National Manager in his responsibility to:*

"Review and assess annually the telecommunications systems security programs and budgets of the departments and agencies of the government, and recommend alternatives, where appropriate, for the Executive Agent and the Steering Group. (NSDD-145, 7j)

"Review annually the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for the Executive Agent and the Steering Group." (NSDD-145, 7k)

- o And collaterally, to support the NTISSC in its responsibility to:

"Submit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities." (NSDD-145, 5b(3))

*Note that while the National Manager, the Executive Agent, and Systems Security Steering Group may be able to review the detailed program and budget proposals of each agency for telecommunication systems security, NSDD-145 provides those groups the authority only to view the aggregate of the program and budget proposals of the agencies for the security of automated information systems. OMB aggregates this data.